Un nemico nel vostro telefono

Victor Chebyshev

Roman Unuchek

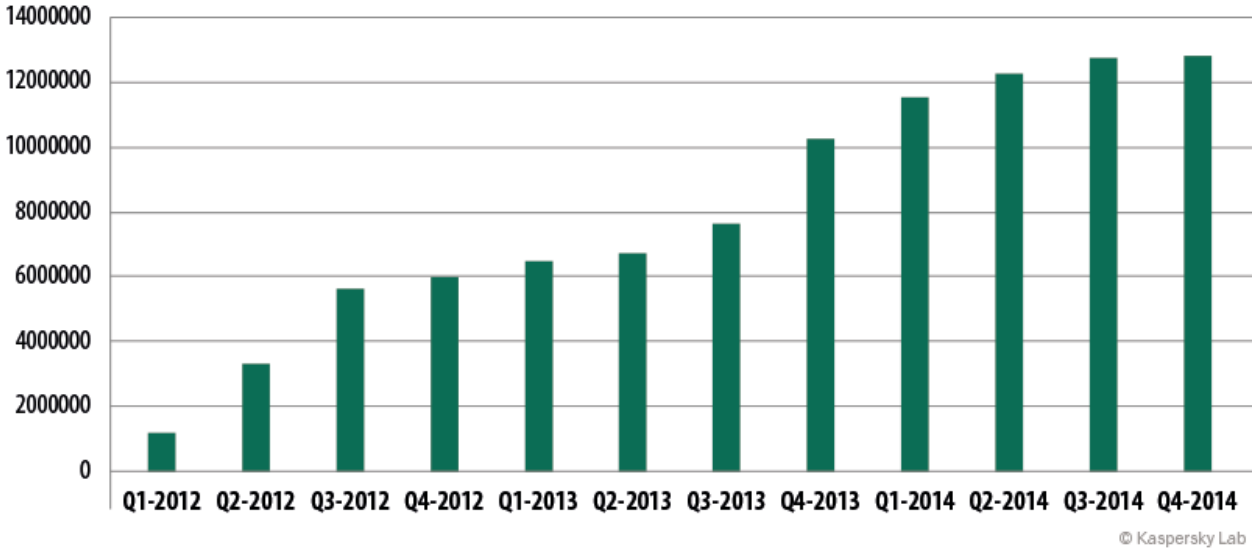
Sommario

In genere, le persone che non possiedono conoscenze specifiche nel settore della sicurezza informatica ritengono, erroneamente, che gli smartphone siano di fatto esenti dalle temibili infezioni provocate dai programmi malware. Soltanto qualche anno fa, a dire il vero, la situazione era proprio quella sopra descritta, visto che gli sviluppatori delle piattaforme mobile, sin dalle fasi iniziali, avevano ben pensato di dedicare tutte le necessarie attenzioni al tema della sicurezza informatica, cercando di conferire ai propri prodotti il massimo livello di protezione nei confronti dei software nocivi. In sostanza, i sistemi operativi mobile non consentivano ai programmi nocivi di acquisire agevolmente il controllo del dispositivo preso di mira.

Con il passare del tempo, purtroppo, la situazione è radicalmente cambiata, soprattutto a causa della crescente espansione delle infinite possibilità tecniche ed operative di cui sono provvisti gli apparati mobile posseduti dagli utenti. Gli smartphone attuali, come tutti sanno, costituiscono per l'utente sia uno strumento di lavoro completo, sia un vero e proprio centro di intrattenimento, nonché un comodo mezzo per gestire le proprie finanze personali. E quanto più elevato è il numero delle attività che lo smartphone è in grado di svolgere, tanto maggiori saranno le subdole attenzioni ad esso dedicate dai malintenzionati, i quali, ovviamente, non si pongono mai troppi scrupoli nel ricavare considerevoli profitti illeciti a spese degli altri; la naturale conseguenza di tutto ciò, nel torbido panorama delle minacce informatiche, è il repentino aumento del numero delle applicazioni nocive appositamente sviluppate per attaccare i dispositivi mobile, così come la rapida espansione della già vasta gamma di metodi e trucchi escogitati dai criminali per realizzare il processo di diffusione ed installazione del malware mobile sui dispositivi-vittima.

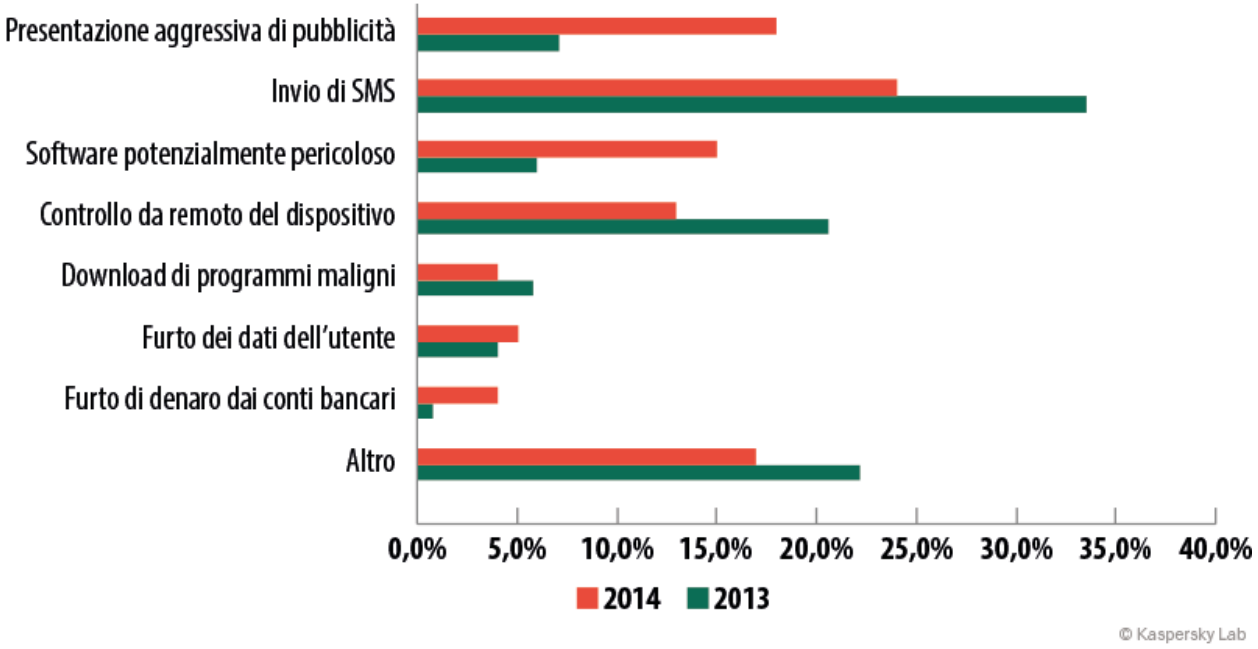
Di conseguenza, naturalmente, si registra un continuo ed esponenziale aumento del numero dei Trojan mobile presenti sulla scena del malware. Le dinamiche di tale fenomeno sono a dir poco impressionanti:

infatti, rispetto al primo trimestre dell'anno 2012, il numero complessivo dei malware mobile risulta cresciuto di oltre dieci volte, ed è così andato a superare, nel quarto trimestre del 2014, la fatidica soglia dei 12 milioni di esemplari.



Numero complessivo di pacchetti di installazione maligni rilevati nel periodo 2012-2014

Desideriamo ugualmente porre in risalto come sia significativamente cambiata anche la ripartizione per tipologia dei programmi dannosi destinati ai dispositivi mobile, in base alle diverse funzionalità espletate da tali software nocivi. Il grafico qui sotto inserito evidenzia, in primo luogo, come i tradizionali Trojan-SMS ed i programma backdoor multifunzionali stiano attualmente cedendo il passo ai malware pubblicitari ed ai Trojan bancari. È, tuttavia, doveroso sottolineare come la diminuzione della quota percentuale inerente ai programmi nocivi riconducibili ad una certa tipologia, non significhi affatto che questi ultimi siano destinati a scomparire progressivamente dalla scena; l'elemento di primaria importanza è effettivamente rappresentato dall'evidente crescita del numero complessivo di programmi maligni appositamente sviluppati dagli autori di malware per attaccare i dispositivi mobile.



Ripartizione dei malware mobili in base alle diverse funzionalità da essi possedute (file presenti nella "collezione" di Kaspersky Lab)

Ovviamente, i virus writer di ogni latitudine non sfornano i propri Trojan in quantità così elevate giusto per fare collezione degli stessi, né tantomeno per vantarsi poi, nell'ambito dei numerosi forum underground esistenti in Rete, del fatto di essere stati in grado di realizzare software nocivi sempre più temibili. Le "creature" malvagie prodotte dai cybercriminali sotto forma di pericolosi malware, in realtà, sono tutte quante in condizione di mirare al bersaglio prefissato, di "scovare" perfettamente le proprie vittime, e non solo: a volte si può addirittura trasecolare quando ci si rende conto di quanto facilmente, e con quali metodi tutt'altro che astuti, i malware in questione possono penetrare all'interno dei dispositivi mobili.

Una sorta di «fai-da-te»

Che ci crediate o no, sono gli stessi utenti a causare il processo di infezione degli apparati mobile da essi posseduti.

E' ormai ben noto come un programma maligno possa insinuarsi all'interno di un computer a totale insaputa del suo proprietario. La procedura è piuttosto semplice: vi recate, ad esempio, su un sito web da voi conosciuto, particolarmente frequentato dal pubblico della Rete; supponiamo che il sito in questione sia stato precedentemente violato da ignoti malintenzionati: sul vostro browser, in qualche frame ben nascosto alla vostra visione, si apre un sito nocivo, dopodiché, con l'ausilio di un vero e proprio arsenale di exploit, viene generato il download, sul vostro computer, ed a vostra totale insaputa, di qualche pericoloso programma malware.

Sulle piattaforme mobile, invece, l'infezione informatica si propaga in maniera del tutto diversa. Infatti, grazie alle stesse caratteristiche tecniche ed ai principi sui quali si basano tali sistemi operativi, quasi nessuna vulnerabilità potrà mai essere d'aiuto agli hacker per poter agevolmente penetrare all'interno del vostro dispositivo mobile, senza il vostro consenso e, soprattutto, senza che ve ne possiate in

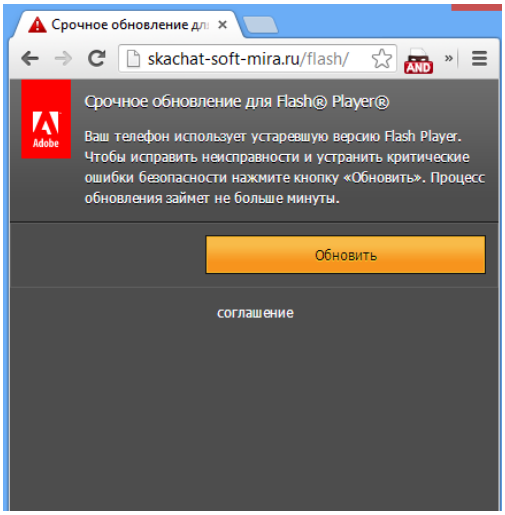
qualche modo accorgere. In pratica, dovreste essere proprio voi a generare l'installazione e la successiva esecuzione di qualche insidioso Trojan mobile, o di un altro pericoloso malware, sul vostro smartphone o tablet, proprio come recita la famosa storiella del primo virus ("prego, eliminare tutti i dati importanti e riformattare il disco rigido").

Il meccanismo di cui si avvalgono gli utenti per effettuare l'installazione dei programmi sul proprio dispositivo rappresenta, ad ogni caso, uno dei punti deboli e teoricamente vulnerabili delle piattaforme mobile, soprattutto per quel che riguarda il sistema operativo Android. Con l'iOS risulta piuttosto arduo installare un programma che non provenga dall'App Store, il noto negozio di applicazioni della casa di Cupertino, mentre Android permette la realizzazione di tali procedure apponendo un semplice segno di spunta nelle impostazioni. Il sistema operativo simboleggiato dal piccolo robot verde verifica, ad ogni caso, la firma digitale che correda il pacchetto di installazione; questo, in teoria, dovrebbe proteggere il dispositivo mobile dall'eventuale attacco di programmi maligni. In realtà, purtroppo, per la piattaforma Android non esiste ancora alcuna autorità di certificazione; nessuno, di fatto, provvede a controllare l'identità del proprietario della firma. Per tale motivo, i malintenzionati non fanno altro che firmare il proprio programma con una qualsiasi firma digitale; l'installazione del software dannoso avviene così senza problemi di sorta, purchè, ovviamente, l'operazione risulti essere consentita da parte dell'utente.

E sono davvero in molti coloro che forniscono il proprio assenso all'installazione di programmi di origine sconosciuta. Il fatto è che appare indubbiamente molto più semplice premere il tasto OK sullo schermo, all'interno dell'apposita finestra in cui si richiede l'assenso per effettuare l'installazione, anziché procedere ad un'attenta riflessione sul tipo di attività che sta per essere eseguita sul proprio dispositivo mobile.

L'utente ordinario raramente si preoccupa delle delicate e complesse questioni legate alla sicurezza IT, tematica piuttosto distante dal comune pensare di tutti i giorni. E poi, è sempre una grande tentazione il poter acquistare un programma utile, oppure un gioco particolarmente interessante e divertente, così come avere la possibilità di effettuare download gratuiti attraverso uno dei tanti siti web preposti a tale servizio. L'applicazione scaricata sul proprio dispositivo, verosimilmente, sembrerà a tutti gli effetti funzionare secondo le migliori aspettative... mentre il denaro presente sul proprio account mobile inizia a scomparire ad una velocità da capogiro, mentre la propria carta di credito viene progressivamente svuotata... Ed ancora: se un sito web particolarmente interessante propone la visione gratuita di qualche

allettante video (e richiede soltanto di aggiornare Flash Player!), dove potrà mai nascondersi la tanto temuta minaccia?



Pagina web fasulla, in cui si propone l'aggiornamento di Adobe Flash Player. L'utente viene informato del fatto che la versione del programma di cui egli dispone è ormai obsoleta e necessita quindi dell'indispensabile aggiornamento.

L'utente non particolarmente esperto non sa, di fatto, che sullo smartphone i programmi non vengono aggiornati con le stesse procedure comunemente adottate per i computer; da parte loro, i malintenzionati possono propinare all'utente qualsiasi cosa loro convenga, sotto l'apparente forma di un indispensabile aggiornamento per un'applicazione mobile di indubbia utilità.

I cybercriminali, come è noto, dimostrano molto spesso di essere estremamente determinati, tenaci ed astuti nel raggiungimento dei loro loschi obiettivi: in genere, le applicazioni nocive per dispositivi mobili vengono da essi diffuse sotto le mentite spoglie dei più svariati programmi utili, giochi, video porno o fantomatici player per la visualizzazione di contenuti pornografici.

Ecco come è possibile imbattersi sul malware

Visto che, in pratica, è l'utente stesso ad installare il programma dannoso sul proprio smartphone, i malintenzionati fanno tutto il possibile per attirare la potenziale vittima verso un sito web dannoso dal quale verrà poi subdolamente eseguito il download del software nocivo. Per far ciò i cybercriminali ricorrono, in particolar modo, alla pratica del cosiddetto "black SEO" - in sostanza una Search Engine Optimization falsata, un metodo illecito utilizzato per innalzare in maniera scorretta il ranking di un sito web nell'ambito dei risultati restituiti da un motore di ricerca; in tal modo i malintenzionati riescono di frequente a far comparire link pericolosi al top della graduatoria dei siti Internet proposti dal search engine. Una volta che il ranking del sito maligno ha raggiunto il posizionamento desiderato, i cybercriminali sono di fatto pronti a procedere all'auspicato "raccolto".

Supponiamo che un utente mobile - magari un po' annoiato durante la sessione di navigazione condotta in Rete - vada ad inserire, nell'apposita casella di ricerca del search engine preferito, la query "download giochi per Android", e veda poi comparire, nella prima o nella seconda riga dei risultati proposti dal motore di ricerca, un link ad un sito web che, presumibilmente, sembra

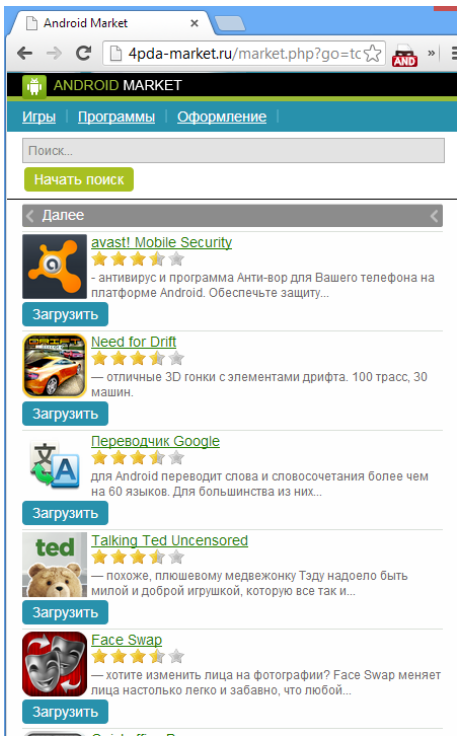
davvero contenere i giochi richiesti; le tanto agognate applicazioni per l'intrattenimento sullo smartphone potrebbero però rivelarsi essere, in realtà, non tanto giochi semplici ed ordinari, bensì giochi "con sorpresa", una sorpresa... quantomai sgradita. È ormai risaputo come il vasto pubblico dei navigatori Internet tenda, quasi naturalmente, a riporre la propria fiducia, in primo luogo, nei siti che appaiono sulle prime righe della pagina web contenente i risultati restituiti dal motore di ricerca. L'utente è portato a ritenere, in genere, che se un sito viene frequentato da migliaia di persone, esso possa sicuramente contenere i giochi o i programmi che fanno all'occorrenza. Non si pensa, invece, alla sicurezza; il che, ovviamente, è un grave errore.

Spesso, per innalzare il ranking di un sito web al top dei risultati prodotti dal motore di ricerca, i malintenzionati fanno illecitamente ricorso alle botnet, o "reti-zombie" che dir si voglia: migliaia di bot, dispiegati dai cybercriminali, introducono su Google e Yandex determinate query di ricerca, per poi andare a finire sul sito malevolo di cui i criminali intendono avvalersi per diffondere i programmi malware di loro interesse; in tal modo viene artificialmente innalzata la posizione del sito Internet in causa nell'ambito dei risultati via via restituiti dai search engine. Inoltre, i link preposti a condurre verso la pagina web maligna allestita dai criminali informatici vengono di frequente pubblicati all'interno dei più disparati forum, sulle bacheche di annunci online, oppure vengono addirittura posizionati tra i commenti che gli utenti inseriscono quotidianamente sui vari siti di news. È qui che vengono poi individuati dai crawler dei motori di ricerca; ne consegue che il ranking dei siti web nocivi viene ulteriormente innalzato, "gonfiato" in maniera del tutto innaturale.

D'altra parte, non si può certo dire che i search engine non conducano un'accanita lotta nei confronti di tali metodi di "ottimizzazione" illegale del rating dei siti dannosi. Li combattono vigorosamente, certo, bloccando l'accesso a decine, centinaia di siti dannosi. Questa risoluta azione da parte dei motori di ricerca, tuttavia, non sembra turbare più di tanto i sonni dei malintenzionati della Rete: i cybercriminali, di fatto, creano e "promuovono" costantemente nuovi siti web, avvalendosi di strumenti automatizzati.

Un ulteriore metodo, ampiamente utilizzato dagli hacker per cercare di attirare un cospicuo numero di utenti mobile verso i siti preposti alla distribuzione di applicazioni nocive, è rappresentato dallo spam via SMS. Si può ad esempio trattare di una mailing di massa volta a diffondere messaggi contenenti link in grado di condurre il potenziale destinatario-vittima verso una determinata risorsa web maligna; naturalmente, i malintenzionati confidano proprio sul fatto che qualcuno vada a cliccare sul link nocivo inserito nell'SMS. Un'azione dannosa ancor più efficace e redditizia per i cybercriminali viene indubbiamente svolta da quelle mailing di massa generate grazie al dispiegamento dei famigerati worm SMS. È sufficiente che un simile programma malware penetri all'interno dello smartphone di un qualsiasi utente per scatenare poi l'invio di messaggi SMS - contenenti un determinato link nocivo - verso tutti i nominativi presenti nell'elenco dei contatti custodito nel dispositivo mobile di cui è proprietario l'utente preso di mira. Abitualmente, un messaggio proveniente da una persona conosciuta non suscita alcun tipo di sospetto, soprattutto quando il testo appare pienamente credibile; questo fa sì che siano in molti coloro che, effettivamente, cliccano sul link inserito nell'SMS appena ricevuto, aspettandosi di vedere, magari, delle foto personali, oppure qualche ottimo esempio di umorismo della Rete, presumibilmente condiviso da qualcuno della propria cerchia di "amici". Aprendo il relativo sito web dannoso, tuttavia, l'utente-vittima riceverà, in veste di gradito ed inatteso "regalo", un pericoloso software nocivo.

Desideriamo segnalare, inoltre, ancora un ulteriore metodo ampiamente utilizzato dai malintenzionati per coltivare i propri loschi interessi, sfruttando in maniera decisamente parassita l'elevato livello di popolarità raggiunto - tra lo sterminato pubblico della Rete - da determinati siti web del tutto legittimi. Nella circostanza, gli hacker provvedono innanzitutto a violare certe risorse Internet, abitualmente frequentate da una moltitudine di navigatori del web: si tratta, più precisamente, di celebri siti di news, famosi negozi online, noti portali a tema. Così, se il software presente nel sito contiene delle vulnerabilità note ai cybercriminali, questi ultimi provvedono ad iniettare codice nocivo all'interno di una o più delle pagine web di cui la risorsa Internet si compone, codice maligno il cui scopo sarà principalmente quello di reindirizzare i visitatori del sito compromesso verso un altro sito web, imbottito di programmi malware. E se poi i malfattori non individuano alcuna vulnerabilità, e non possono quindi sfruttare le eventuali falle di sicurezza, essi potranno sempre cercare di sottrarre illecitamente le credenziali dell'amministratore del sito sottoposto ad attacco; per ottenere ciò, i cybercriminali di turno non mancheranno certo di ricorrere a subdole pratiche di phishing, oppure allo sfrontato utilizzo di (più o meno) astute tecniche di ingegneria sociale. In caso di esito positivo dell'azione criminosa svolta, i malfattori saranno in grado, in pratica, di fare del sito ciò che più desiderano, fino, ovviamente, a collocare all’interno dello stesso un vero e proprio arsenale di pericolosi programmi nocivi.



Screenshot relativo ad un Android Market fasullo

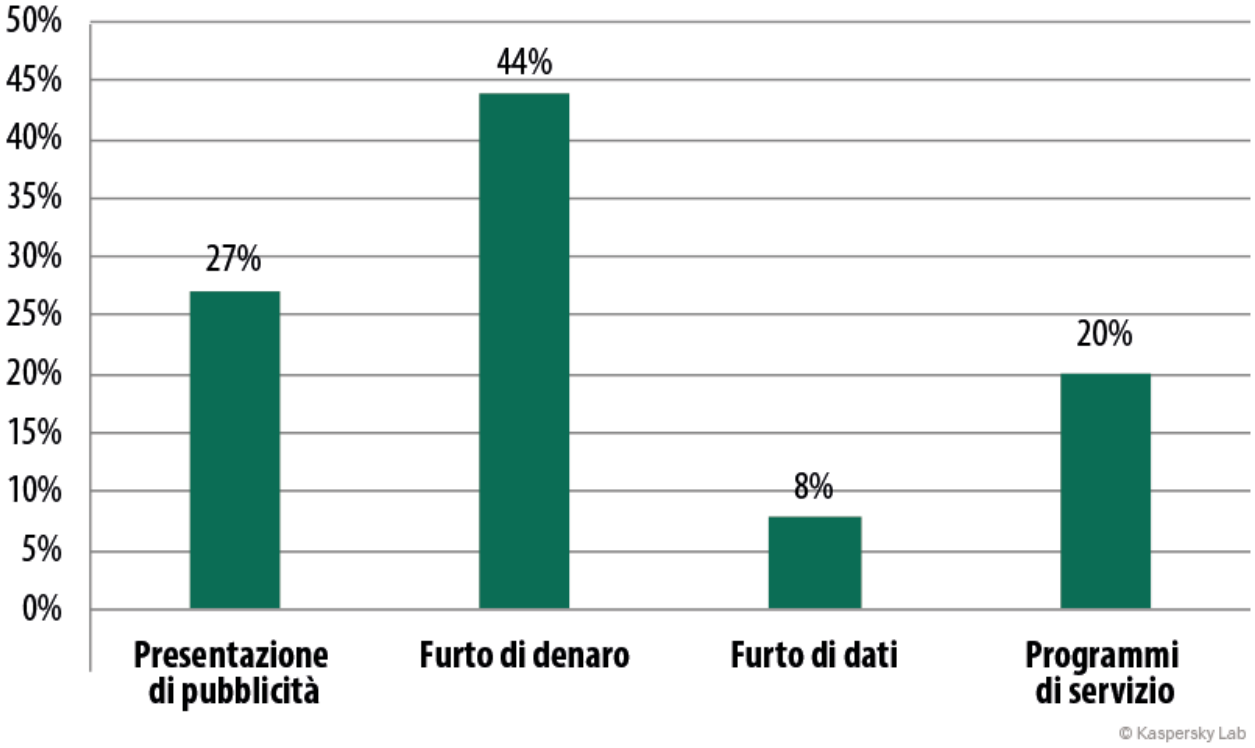
I programmi nocivi destinati a colpire i dispositivi mobile, oltre ai metodi sopra descritti, vengono a volte diffusi tramite un metodo che potremmo paradossalmente definire “quasi onesto", cioè attraverso gli app store, i negozi virtuali che permettono agli utenti di scaricare e acquistare le innumerevoli applicazioni via via rese disponibili dagli sviluppatori. Può magari trattarsi di un programma legittimo nel quale è stato iniettato del codice nocivo, oppure di un'applicazione dannosa appositamente sviluppata dai virus writer, preposta a simulare l'esecuzione di qualche funzione di particolare utilità, oppure, perché no, di un temibile malware "nudo e crudo", semplicemente mascherato dai suoi autori per mezzo di un nome ed un'icona fasulli.

Screenshot relativo ad un falso Google Play

In genere, tali programmi vengono scaricati attraverso gli app store non ufficiali, negozi di applicazioni che spesso trascurano del tutto le più elementari regole e procedure di protezione IT, oppure non controllano in maniera accurata ed adeguata i contenuti proposti, limitandosi, di frequente, alla semplice esecuzione di una scansione antivirus automatica. Esistono ad ogni caso alcuni precedenti in cui tali programmi dannosi sono stati collocati da ignoti malintenzionati all'interno dei negozi online ufficiali preposti alla distribuzione di applicazioni per dispositivi mobile e di numerosi altri contenuti digitali: tale situazione si è in effetti verificata sia con Google Play, sia con l'App Store di Apple, negozio tradizionalmente ancor più protetto. Le varie aziende, naturalmente, provvedono prontamente ed efficacemente a "ripulire" i propri negozi di applicazioni; il fatto è che, tuttavia, i malintenzionati non se ne stanno certamente a guardare con le mani in mano.

È così che si arricchiscono i cybercriminali «mobile»

Una volta insediatosi nel vostro smartphone, il programma maligno inizia subito a svolgere il compito per il quale è preposto: riempire di denaro le tasche del proprio "padrone". E tutto questo, naturalmente, a vostre spese! I dispositivi mobile presenti attualmente sul mercato rappresentano, per i malintenzionati informatici, una sorta di vero e proprio Klondike; l'elemento di fondamentale importanza, per tali malfattori, è indubbiamente quello di essere in grado di sfruttare "a dovere" una simile (potenziale) "miniera d'oro".



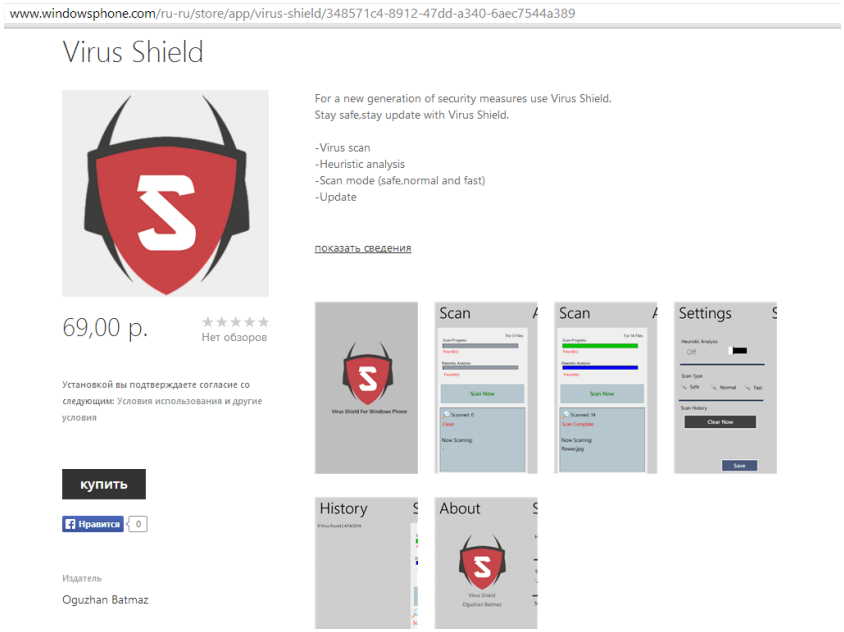
Malware mobile: i principali metodi di "monetizzazione"

Trucchi e furberie a caro prezzo

Il metodo più "innocente" attualmente utilizzato dai truffatori "mobile" consiste nel presentare réclame di ogni genere agli utenti, in maniera a dir poco aggressiva e insistita. E' vero che tutto ciò non può arrecare particolari danni ai proprietari dei dispositivi; tuttavia, le notifiche pop-up che compaiono periodicamente sullo schermo, contenenti i più disparati banner pubblicitari, iniziano molto presto ad

infastidire seriamente l'utente-vittima. Per di più, sbarazzarsi di queste poco gradite "apparizioni", propinate in maniera forzata ed ossessiva, non è affatto cosa semplice; risulta in effetti davvero difficile poter determinare quale sia il programma preposto allo svolgimento delle attività indesiderate in questione! È forse possibile che si tratti di Angry Birds HD, oppure di qualcos'altro dal nome del tutto impronunciabile, magari camuffato, all'interno del dispositivo mobile, in veste di applicazione di sistema.

Meritano poi una menzione a parte quelle applicazioni fasulle la cui attività non produce in genere nulla di buono o di utile, ma nemmeno nulla di dannoso; tali applicazioni, tuttavia, possono talvolta costare quasi un occhio della testa agli utenti più disattenti od inesperti. Alcune di esse, in pratica, sono delle vere e proprie scatole vuote, subdolamente collocate nelle sezioni a pagamento degli app store; ne costituisce un più che "valido" esempio quel programma che promette di rendervi rapidamente ricchi, ma che in realtà non fa null'altro se non mostrare l'immagine di un diamante sullo schermo del vostro smartphone. Altre ancora si mascherano sotto forma di qualcosa di utile, ad esempio nelle vesti di un programma antivirus, che richiede all'utente mobile l'effettuazione di micropagamenti per proteggersi nei confronti di non ben definiti programmi Trojan, i quali, in apparenza, avrebbero contagiato il dispositivo dell'utente.



Guadagnare dal telefono

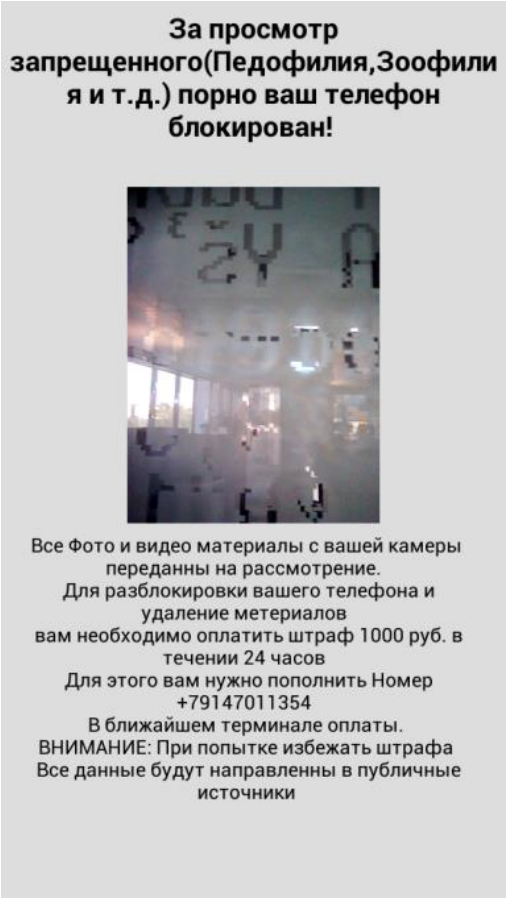
Il metodo più classico utilizzato dai malintenzionati per cercare di ricavare cospicui profitti attraverso il dispiegamento di malware mobile è tuttora rappresentato dall'invio di SMS verso numeri premium, ovvero costosi numeri a pagamento. Nella fattispecie, un determinato programma Trojan, insediatosi all'interno del telefono preso di mira, si mette semplicemente ad inviare vari messaggi SMS a pagamento, svuotando in tal modo l'account mobile dell'utente. L'operatore di telefonia mobile provvederà quindi a trasferire il relativo denaro dal vostro account all'account del locatario del numero premium (il malintenzionato di turno), non rilevando in tale operazione nulla di illegale, visto che i numeri premium, al momento attuale, continuano a rappresentare un metodo alquanto diffuso per effettuare il pagamento di numerosi servizi erogati in Internet.

Un ulteriore metodo ampiamente praticato dai cybercriminali per tentare di guadagnare alle spalle dei proprietari degli smartphone infettati dal malware è poi costituito dal furto dei dati sensibili, ovvero i dati particolarmente preziosi ed importanti per l'utente-vittima. Nel vostro elenco dei contatti, nei messaggi SMS custoditi sul vostro smartphone, così come all'interno della posta elettronica si possono

trovare cose davvero molto interessanti, per i malintenzionati. Potreste così contribuire, come minimo, ad arricchire i database quotidianamente utilizzati dagli spammer per l'invio di montagne di fastidiose e-mail indesiderate, mentre i dispositivi mobile dei vostri amici e conoscenti potrebbero essere invasi, a loro volta, da messaggi pubblicitari ed insidiosi link nocivi. E se, per esempio, avete inviato o ricevuto tramite posta elettronica le credenziali occorrenti per l'amministrazione di un qualsiasi sito web, senza preoccuparvi di modificare poi le stesse, state pur certi che i criminali, in caso di attacco informatico nei vostri confronti, apprezzeranno tutto ciò in maniera particolare, e saranno quindi ben lieti di accogliere il vostro sito web "in famiglia".

Smartphone o portafoglio?

Hanno recentemente fatto la loro comparsa, sui dispositivi mobile, anche i cosiddetti Trojan "estorsori", programmi dannosi già ampiamente diffusi nel mondo dei computer. Il loro schema di funzionamento è molto semplice: tali malware, una volta insediatisi all'interno del vostro dispositivo, fanno sì che sullo schermo dello smartphone preso d'assalto venga mostrata una particolare foto accompagnata da contenuti minacciosi, con tanto di effettiva richiesta di riscatto. L'utente-vittima, nel frattempo, non può più operare in alcun modo sul proprio dispositivo, in quanto il funzionamento dello stesso risulta bloccato. Tutto ciò che si può fare, per risolvere al più presto l'incresciosa ed inaspettata situazione, è inserire un particolare codice, di cui si promette l'invio non appena sarà stato effettuato il pagamento di una determinata somma di denaro.



Il messaggio che il Trojan estorsore fa comparire sullo schermo del dispositivo mobile recita così: «A seguito della visualizzazione di contenuti proibiti di natura pornografica (Pedofilia, Zoofilia, etc.) il suo telefono è stato bloccato! Tutte le foto ed i materiali video custoditi nello smartphone sono già stati opportunamente trasferiti per essere sottoposti agli esami del caso. Per procedere all'operazione di sblocco del telefono e alla rimozione di tali materiali dovrà essere necessariamente pagata una multa di 1.000 rubli, entro le prossime 24 ore. Per fare quanto richiesto è necessario comporre il numero XXXX presso il terminale di pagamento più vicino. ATTENZIONE! Qualora si cerchi di evitare il pagamento della suddetta sanzione, tutti i dati saranno immediatamente trasmessi a fonti pubblicamente accessibili»

Rimuovere il Trojan dal dispositivo infetto risulta peraltro impossibile se non viene eseguito un reset completo delle impostazioni e del contenuto presente nella memoria flash dello smartphone. L'eventuale perdita dei dati memorizzati sul dispositivo può tuttavia rivelarsi talmente dolorosa al punto da spingere alcune vittime dell'attacco informatico del Trojan estorsore ad effettuare il pagamento richiesto quasi senza batter ciglio; in effetti, sborsare la cifra pretesa dai malfattori per procedere allo sblocco del telefono si rivela talvolta essere, paradossalmente, un'azione meno deleteria rispetto al doversi privare di tutta una serie di dati di notevole importanza. Occorre ad ogni caso tener ben presente il fatto che, una volta ricevuti i soldi richiesti, non sempre, anzi piuttosto di rado, i malintenzionati procedono poi all'invio del codice da utilizzare per le operazioni di sblocco del dispositivo mobile.

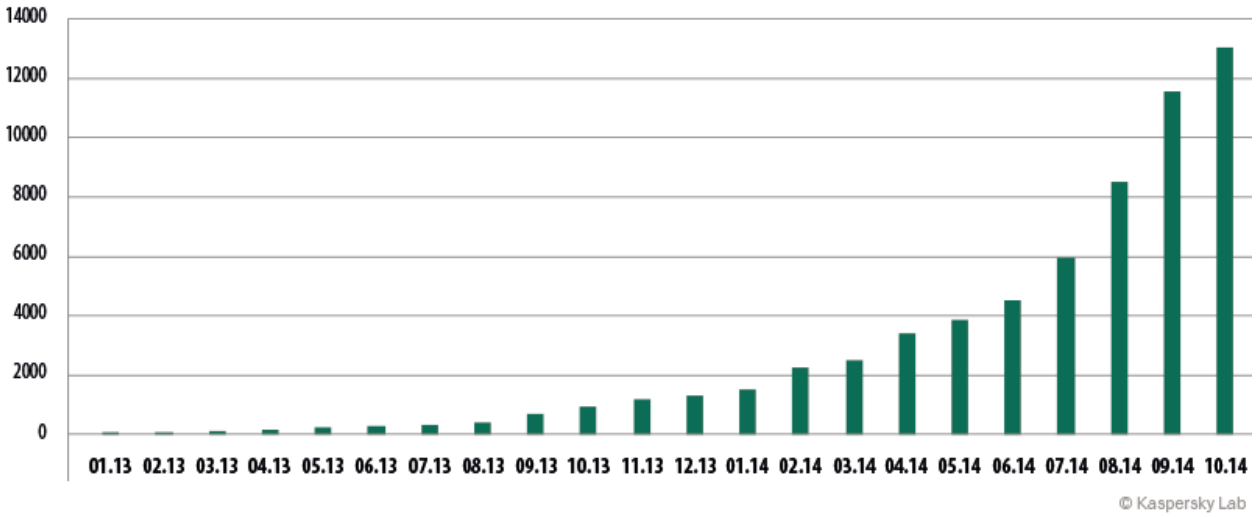
La chiave che apre le porte della vostra banca

Tutti i metodi sopra descritti, tuttavia, appaiono quasi alla stregua di semplici birichinate o poco più, rispetto ad un ulteriore metodo, relativamente nuovo, e ben più efficace e aggressivo, attualmente utilizzato dai cybercriminali per guadagnare sfruttando illecitamente i dati sensibili di natura finanziaria carpiti attraverso i dispositivi mobile degli utenti. Come è noto, in questi ultimi anni hanno conosciuto

una diffusione piuttosto ampia i servizi di mobile banking. Ogni istituto bancario che si rispetti ha quindi sviluppato una propria applicazione mobile, che permette di fatto, alla clientela, di poter gestire le proprie risorse finanziarie tramite il semplice utilizzo dello smartphone - o ha perlomeno provveduto ad introdurre un apposito servizio di banking via SMS.

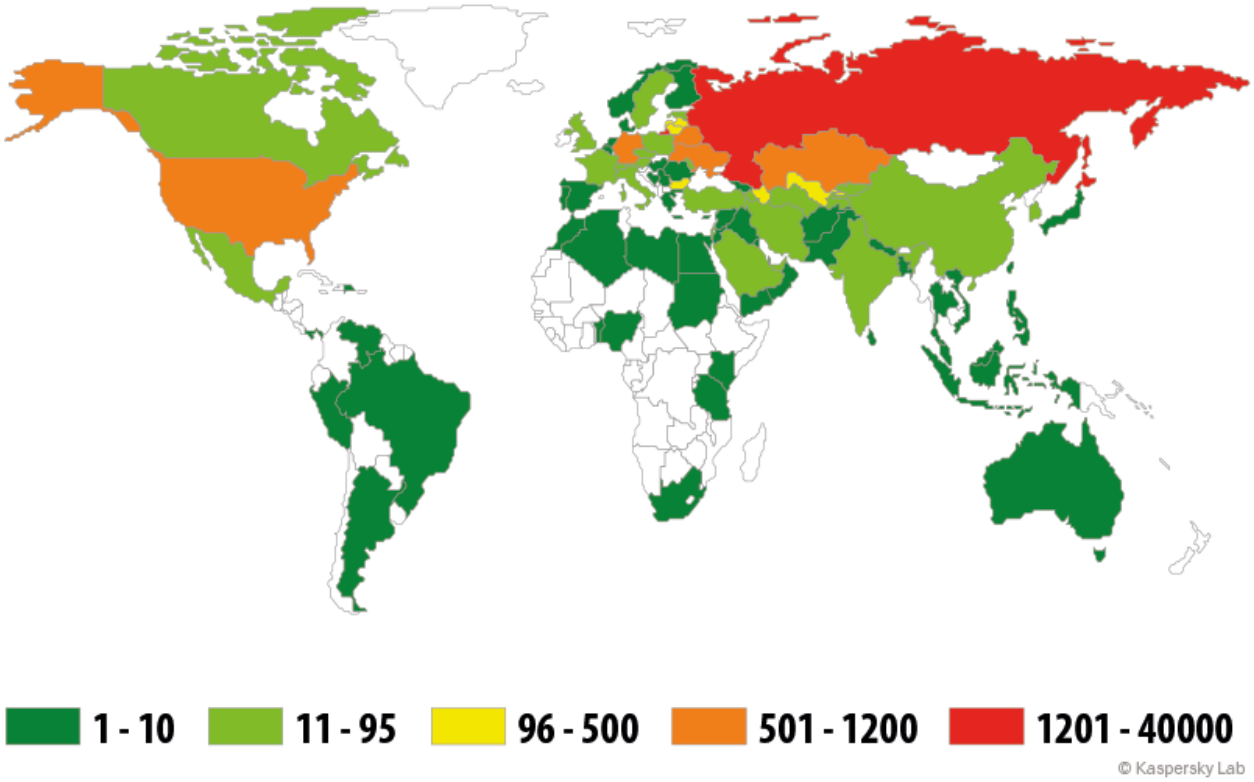
La conseguenza è che, potenzialmente, gli smartphone appartenenti ad un elevato numero di utenti rappresentano delle vere e proprie "chiavi" per l'accesso al conto bancario posseduto da questi ultimi - in certi casi persino a vari conti bancari. Ovviamente, la portata dei possibili profitti ricavati in tal modo dai malintenzionati non può essere ancora comparata ai cospicui guadagni illeciti ottenuti attraverso i metodi criminali classici; tale situazione sembra tuttavia spingere e motivare in particolar modo i cybercriminali proprio nel dirigersi sempre più impetuosamente e rapidamente verso la conduzione di un numero sempre maggiore di attacchi informatici nei confronti dei sistemi di mobile banking.

I dati statistici da noi raccolti delineano, a tal riguardo, un quadro ben chiaro della situazione e dimostrano, in tutta evidenza, quanto sia attualmente elevato e pressante l'interesse nutrito dai virus writer mobile nei confronti dei nostri account bancari. Difatti, mentre all'inizio del 2013 il numero dei Trojan bancari presenti all'interno della nostra "collezione" non raggiungeva neppure il centinaio di unità, nel mese di ottobre 2014 la quantità complessiva di simili software nocivi ha addirittura superato i tredicimila esemplari.



Numero di Trojan bancari per piattaforme mobili individuati nel periodo gennaio 2013 – ottobre 2014

I famigerati Trojan-banker stanno attualmente trovando una diffusione sempre più ampia in numerose parti del mondo; è in Russia, tuttavia, che si osserva, ora come ora, un vero e proprio boom dei banker mobili. Proprio entro i confini della Federazione Russa, tra l'altro, i virus writer si dedicano al "collaudo" delle loro creazioni, prima che le stesse vengano utilizzate in altri paesi.



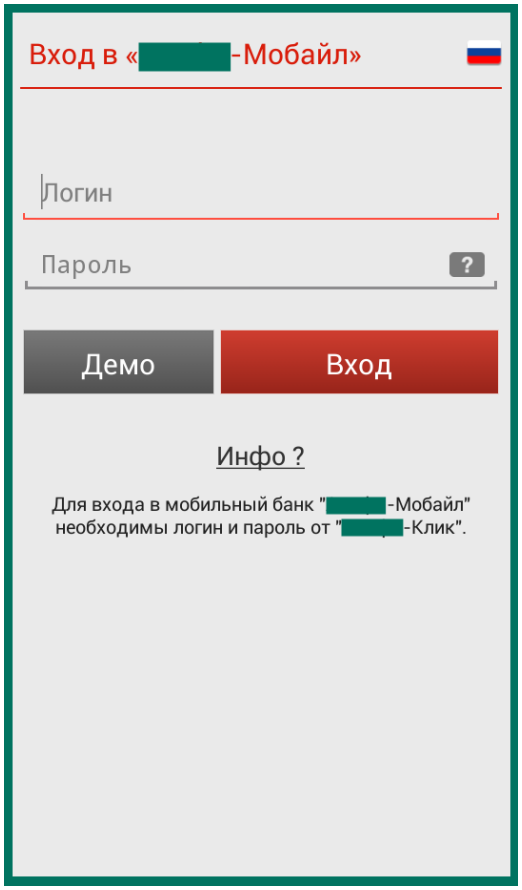
Geografia delle minacce IT per dispositivi mobili dedicate alla sfera bancaria - Periodo: gennaio - ottobre 2014 (numero di tentativi di installazione di Trojan bancari mobili)

La soluzione più semplice ed agevole, per i malintenzionati, per cercare di sottrarre cospicue somme di denaro agli utenti, è rappresentata dal banking via SMS. Per condurre attività criminose in tal senso non si rivelano necessari nemmeno nuovi strumenti, infatti, i malfattori possono tranquillamente ed ottimamente usare gli abituali ed ordinari Trojan-SMS. Il fatto è che numerose banche ritengono, quasi "per impostazione predefinita", che il telefono del cliente sia un mezzo attendibile e, pertanto, accettano le disposizioni inviate dai loro clienti tramite semplici SMS senza condurre procedure aggiuntive di autenticazione. Di conseguenza, il cliente può inviare importi di denaro dal proprio conto bancario sia verso l'account mobile di cui egli è titolare, sia verso account telefonici mobile appartenenti ad altre persone. Sfruttando tale opportunità, i malintenzionati provvedono ad inviare appositi SMS, nella forma appropriata, allo scopo di trasferire il denaro dal conto della vittima verso i propri account; attraverso questi ultimi non risulterà poi affatto difficile monetizzare gli importi illecitamente sottratti, proprio in ragione dell'attuale livello di sviluppo dei sistemi di pagamento mobile.

Spesso, poi, i Trojan bancari mobile operano in simbiosi con gli analoghi programmi Trojan destinati al mondo dei computer; il malware Faketoken, ad esempio, rappresenta perfettamente una di tali "combinazioni" cybercriminali. Così, se il proprio computer è stato infettato da un banker e si accede al proprio account di Internet banking, il malware in questione si attiva, mostrando all'utente la pressante richiesta di effettuare il download di un'applicazione per l'OS Android, la quale viene descritta come del tutto indispensabile ed irrinunciabile per poter garantire in piena sicurezza la conferma della transazione finanziaria in corso. In tal modo, l'utente eccessivamente fiducioso non fa altro che realizzare, sul proprio smartphone, l'installazione del pericoloso programma maligno denominato Faketoken. A questo punto entra in gioco la tecnologia dannosa: il software nocivo che opera sul computer effettua il furto di login e password, cosicché i malintenzionati ottengano agevolmente l'accesso al conto bancario dell'utente-vittima. Essi conducono poi la transazione finanziaria, nel corso della quale Faketoken

intercetta il codice monouso mTAN utilizzato per confermare l'operazione in corso, codice abitualmente inviato dalla banca tramite un apposito messaggio SMS. Il risultato di tutto ciò è che il beneficiario dell'intera somma illecitamente carpita, trasferita dal conto bancario dell'utente, sarà il criminale di turno, il quale provvederà poi a trasformare in contanti, attraverso il bancomat, l'importo sottratto. Sono stati da noi individuati attacchi informatici, condotti mediante l'utilizzo del malware sopra menzionato, in ben 55 diversi paesi, tra cui Germania, Svezia, Francia, Italia, Gran Bretagna e Stati Uniti.

Un terzo metodo per ricavare profitti illeciti è rappresentato dall'utilizzo di Trojan-banker mobile in grado di agire in maniera del tutto indipendente, i quali, in genere, riescono a camuffarsi sotto forma di applicazioni dedicate al mobile banking, oppure, più semplicemente, provvedono a sostituire l'interfaccia dell'applicazione normalmente utilizzata dall'utente per svolgere le proprie operazioni bancarie online. In tal modo, il Trojan carpisce login e password, inseriti dallo stesso utente, e provvede poi a trasmettere le informazioni sensibili così ottenute al proprio server di comando. A questo punto, il malintenzionato in agguato, utilizzando i dati bancari intercettati, effettua agevolmente la transazione. È proprio in questi termini che agisce, ad esempio, il famigerato malware denominato Svpeng. Questo Trojan mobile, in sostanza, si sovrappone alle applicazioni legittime utilizzate dai più importanti istituti bancari russi e ucraini; Svpeng apre sullo schermo del dispositivo mobile un'apposita finestra maligna, assumendo perfettamente le vesti di tali applicazioni.



Finestra di phishing volta ad imitare l'interfaccia dell'applicazione originale della banca

Avvalendosi di tali programmi nocivi, i malintenzionati possono, così, su due piedi, impadronirsi di tutti i vostri risparmi, svuotando i vostri conti bancari e chiudendo i depositi da voi sottoscritti in precedenza; i

cybercriminali possono addirittura farvi sprofondare nei debiti, rimuovendo interamente i limiti previsti per il conto di credito.

Non scavarti la fossa da solo

È di particolare interesse osservare come, nei vari Paesi, la quota percentuale relativa alle applicazioni dannose, rispetto al volume totale delle applicazioni per dispositivi mobile installate dagli utenti, presenti evidenti variazioni. Riportiamo qui di seguito, a tal proposito, gli indici relativi ad alcuni Paesi, rilevati nel periodo gennaio - ottobre 2014 (i dati statistici sono stati ottenuti tramite il servizio KSN di Kaspersky Lab, la rete globale di sicurezza implementata attraverso apposite infrastrutture "in-the-cloud"):

Vietnam	2,34%
Polonia	1,88%
Grecia	1,70%
Repubblica Ceca	1,02%
Francia	0,84%
Belgio	0,74%
Cina	0,73%
Ukraina	0,70%
Russia	0,69%
Messico	0,62%
Spagna	0,54%
Bielorussia	0,50%
Iran	0,38%
Svizzera	0,36%
India	0,34%
Canada	0,23%
Germania	0,18%
Brasile	0,17%
Italia	0,09%
Austria	0,07%
USA	0,07%
Hong Kong	0,05%
Nuova Zelanda	0,05%
Norvegia	0,04%
Giappone	0,01%

È indubbiamente interessante ed alquanto singolare il fatto che, in teoria, non risulterebbe particolarmente complesso proteggersi in maniera adeguata nei confronti del sempre più vasto ed intricato panorama delle minacce IT appositamente create dai virus writer per colpire i dispositivi mobile. In effetti, come è noto, gli sviluppatori delle piattaforme mobile hanno curato notevolmente i vari aspetti della sicurezza informatica; possiamo quindi affermare, senza ombra di dubbio, che l'anello più debole della "catena" sia di fatto divenuto proprio l'utente stesso. Ciò si rivela essere, allo stesso tempo, sia un bene che un male. Un male per il semplice fatto che, attualmente, numerosi utenti mobile non sembrano preoccuparsi più di tanto delle delicate e vitali questioni legate alla loro sicurezza IT. Un

bene, invece, in quanto risulta sufficiente seguire alcune semplici raccomandazioni per potersi proteggere adeguatamente nei confronti delle temibili e variegate minacce informatiche descritte in precedenza.

Raccomandiamo pertanto, a tutti gli utenti mobile, di attenersi alle seguenti regole di sicurezza.

- Evitate in primo luogo di manomettere il vostro smartphone. Sì, effettivamente le eventuali operazioni di jailbreak sull'iPhone e le operazioni di root sui dispositivi provvisti di sistema operativo Android possono fornire ulteriori possibilità riguardo all'utilizzo e alla gestione del vostro telefono; al tempo stesso, però, eseguendo tali operazioni, l'utente fa inconsapevolmente scattare una sorta di semaforo verde per i malintenzionati di turno.
- Disabilitate, sul vostro dispositivo Android, l'opzione relativa alla possibilità di consentire l'installazione di programmi di origine sconosciuta, ovvero quelle applicazioni provenienti da fonti non attendibili.
- Procuratevi un efficace software antivirus per dispositivi mobile, in grado di analizzare le applicazioni al momento della loro installazione.
- Cercate di non cliccare sui link presenti nei messaggi SMS, anche se questi ultimi sembrano provenire da persone conosciute.
- Nel caso in cui abbiate già cliccato sul link contenuto nell'SMS appena ricevuto, non fornite in alcun modo il vostro assenso per eventuali download od installazioni che vi vengono proposti sul momento.
- Effettuate l'aggiornamento delle applicazioni installate sul vostro dispositivo mobile scaricando i relativi update esclusivamente attraverso i negozi online ufficiali, e non tramite qualsiasi altro sito web.